TREND MICRO™ PC-cillin™

Internet Security 2004

TREND MICRO™

Quick Start Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Quick Start Guide, which are available from Trend Micro's Web site at:

www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. PCEM01608/30910

Release Date: September 2003

Protected by U.S. Patent No. 5,951,698

The Quick Start Guide for Trend Micro Internet Security is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

For technical support, please refer to Troubleshooting and Contact Information starting on Contacting Technical Support on page 6-2 for technical support information and contact details. Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 1

Welcome to Trend Micro™ Internet Security

Trend Micro Internet Security protects your computer against Internet threats such as viruses, spyware, hackers, and spam. In addition, with Trend Micro Internet Security you can secure your personal information, block unwanted Web sites, and check email for viruses. Trend Micro Internet Security provides a simple interface to access powerful functionality. New features in Trend Micro Internet Security help ensure that all areas of your Internet and network connection are secure.

So called "spam" email (junk email) is a costly and annoying problem. Trend Micro Internet Security contains a powerful anti-spam feature that lets you filter unwanted email.

Trend Micro Internet Security is designed to detect and block spyware. Spyware is often installed alongside programs downloaded from the Internet, and may track information such as the Web sites you visit and the purchases you make from the Internet.

Trend Micro Internet Security also includes Privacy Data Protection. This feature allows you to specify important, personal information that you do not want sent over the Web or in email messages. Trend Micro Internet Security will block and log any attempts to send this data, which can include items such as your credit card number, your home address, or your telephone number.

Additionally, Trend Micro Internet Security includes outgoing (SMTP) email scanning. This protects other users from being infected by an email from your machine, by scanning all messages and attachments before they leave your computer.

The innovative Outbreak Warning System protects your computer against the latest virus outbreaks and security threats. The Outbreak Warning System warns you in advance of new network virus infections and prompts you to update your software to prevent infection.

This chapter contains the following sections:

- Hit the ground running... on page 1-2
- What's new in Trend Micro Internet Security on page 1-3
- Essential getting started tasks on page 1-6
- Installing your software on page 1-7
- Registering and activating Trend Micro Internet Security on page 1-8
- Updating Trend Micro Internet Security on page 1-9
- Safer computing practices on page 1-11
- Upgrading your trial version software on page 1-12

Hit the ground running...

Even before you completely install Trend Micro Internet Security, it checks your main system files for viruses and Trojan horse programs. Then after it's installed, Trend Micro Internet Security helps keep your computer free from infection with a series of pre-defined automated tasks.

What Trend Micro Internet Security does right from the outset

Without having to configure anything, Trend Micro Internet Security will perform the following:

- Check for viruses every time you open, copy, move, or save a file
- Protect against downloading infected files
- Detect and clean Trojans
- Block spyware

- Scan your email messages and attachments as they are being downloaded from the POP3 email server or sent via an SMTP server (if you use the email clients: Microsoft™ Outlook™ 2000 or above, Outlook Express 5.5 or above, Netscape 7.0 or above, or Eudora™ Pro 5.0 or above). Also, scan Webmail attachments and they are being downloaded from a Webmail server (a Webmail server is accessed by a Web browser for example, Microsoft Hotmail™, Yahoo!™ Mail, and AOL™ Mail)
- Protect your computer against attacks from the Internet using the Personal Firewall
- Monitor your Microsoft Word™ and Excel™ sessions for macro viruses, using MacroTrap™, a system that detects macro viruses through heuristics, rule-based methods, rather than through pattern matching
- Check for unknown viruses based on their "behavior", using advanced heuristic technology
- Scan all files on your hard drive according to a default scheduled scan task
- Scan all program files for viruses according to a default scheduled scan task

What you can do with the click of a button:

- Scan every file on your system
- Scan any file from Windows Explorer or My Computer by right-clicking the file icon
- Scan floppy disks
- Check all Word or Excel documents for macro viruses

What's new in Trend Micro Internet Security

As viruses and other malicious programs become stronger and more clever, Trend Micro Internet Security also continues to become more powerful to provide complete personal virus protection and Internet security.

Feature	Description
Privacy Data Protection	This feature allows you to define certain types of information (for example, your name, address, or credit card number) which will then be blocked from being sent over the Web or in email messages.
Anti-spam	Trend Micro Internet Security includes a powerful and customizable anti-spam engine. Email messages identified as spam are tagged for easy filtering or deletion. You can configure an approved senders list (a list of email addresses you know are safe) to ensure important messages are not inadvertently tagged.
Personal Firewall profiles	Depending on your computer and network settings, you may require certain ports or services enabled in some situations or disabled in others. By using Personal Firewall profiles, you can easily switch profiles between, for example, a home network and a wireless LAN, thereby keeping your security as tight as possible.
Spyware scan	Trend Micro Internet Security detects and removes spyware. Spyware is often installed secretly with legitimate programs downloaded from the Internet. Spyware tracks and reports your personal data to a centralized database. Information tracked may include your location, which Web sites you visit, and what you purchase online.
Outgoing SMTP scan	Trend Micro Internet Security scans outgoing SMTP email messages and attachments.

Minimum system requirements

You need the following minimum software and hardware to run Trend Micro Internet Security.

Operating System:

- Microsoft™ Windows™ 98, 98SE, Me, 2000 Professional with Service Pack 3 or later, XP Home or Professional with Service Pack 1 or above

CPU:

- Intel™ Pentium™ 166MHz or equivalent processor for Windows 98, 98SE, Me
- Intel Pentium 300MHz or equivalent processor for Windows 2000, XP

Memory:

- 64MB of RAM (128MB or more recommended) for Windows 98, 98SE, Me, 2000
- 128MB of RAM for Windows XP

For all installations:

- Internet Explorer 5.5 with Service Pack 2 or later
- 100MB of available hard disk space for installation
- Mail Scan supported clients: Microsoft Outlook Express 5.5 or later, Microsoft Outlook 2000 or later, Netscape Messenger 7.0 or later, Eudora Pro 5.0 or later.

Note: Hardware requirement depends on your software environment. An Internet connection is required to perform online registration, update, and other online services.

Essential getting started tasks

This section provides a list of the most important tasks you have to complete to get up and running with Trend Micro Internet Security. To effectively use Trend Micro Internet Security and start protecting your PC, we strongly recommend that you perform all of these tasks.

Task	Topic
Install the software	Refer to *Installing your software* on page 1-7.
Register Trend Micro Internet Security	Refer to *Registering and activating Trend Micro Internet Security* on page 1-8 to register your software and enable updates. Trend Micro Internet Security needs to update pattern and program files to stop the latest viruses.
Perform a Manual Update	Refer to *Updating Trend Micro Internet Security* on page 1-9. As people constantly unleash new viruses, we strongly recommend that you regularly update Trend Micro Internet Security. Enable the Intelligent Update option to let Trend Micro Internet Security automatically update itself.
Manually Scan all files	Refer to *Scanning your entire computer* on page 3-3, to perform a complete scan of your computer to ensure there are no viruses or other malicious programs hiding on your PC.

Installing your software

Installing Trend Micro Internet Security is simple and only takes a few minutes.

Important: Before installation, you must remove any existing antivirus or firewall software, including other Trend Micro antivirus software.

To install Trend Micro Internet Security:

1. Insert the Trend Micro Internet Security program CD into your CD-ROM drive, and do the following:
   - If the menu automatically appears, click **Install Program**, and then click **Next**.
   - If the installation program doesn't automatically start, from the Windows taskbar click **Start** > **Run**. In the **Open** field, type D:\Setup\setup.exe and click **OK** (where D:\ is the drive letter of your CD-ROM). Click **Next**.
2. Click **I accept the terms in the license agreement** to accept and continue installing Trend Micro Internet Security. The installation procedure will quit if you do not accept the terms.
3. Click **Next**. Trend Micro Internet Security scans your system memory, boot sector, and critical files before installing the program files. If Trend Micro Internet Security finds an infected file, it cleans or deletes it. The **Customer Information** screen appears. Do the following:
   - In **User Name**, type a user name. You must provide a user name to continue installation.
   - In **Organization**, type the name of your organization.
   - In **Serial Key**, type your serial key. If you do not have a serial key, you can continue installation and install a 30-day trial version. If you want to install the trial version, an additional screen appears when you click **Next** giving you the option to install it. Select the **I want to install the 30-day trial version** check box, and then click **Next**. With this version you will not be able to register or update and after 30 days virus scanning will be disabled--you should either purchase the product or remove it.

4. Click **Next**. The **Destination Folder** screen appears. You can choose where Trend Micro Internet Security will be installed or use the default location. To change the location click **Change**, and then browse to the desired location.
5. Click **Install** to begin installation.
6. After installation, the wizard informs you that the installation is successful. Click **Finish** to exit the installer.

If the installer needs to reboot the system, close all running programs and click **Yes** to reboot.

Registering and activating Trend Micro Internet Security

Take a few minutes to register your software online and receive the benefits. A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Important: You must register your software before you can perform program and pattern file updates. You need to perform updates to keep your computer protected.

To register Trend Micro Internet Security:

1. Make sure you are connected to the Internet.
2. On the Trend Micro Internet Security main window, click **Update > Registration**.
3. Confirm that your full version serial number already exists and click **Register Now**.
4. On the Register Web page, click **New User Registration** (first-time users), and click **Register Now!**.
5. To activate your product, type your name, email address, and other required information in the appropriate fields and make sure the Customer Care Center check box is selected.

6. Click **Preview**. Confirm the information you entered is correct.
7. Click **Submit**. The New Member Registration Web page appears. Continue to follow the on-screen instructions and reply to the activation email.

You have registered your software and are a Trend Micro Customer Care Center member. You can now download updates to Trend Micro Internet Security.

Note: If you have trouble viewing the Registration page, you may need to configure your proxy settings. Refer to *Enabling and configuring proxy settings* on page A-3 in the Appendix for instructions.

Updating Trend Micro Internet Security

To protect your computer against the latest threats, you need to regularly update your program files, scan engine, and virus pattern files. Updated pattern files are released by Trend Micro on at least a weekly basis. Updating your pattern file provides you with the most up-to-date protection and lets Trend Micro Internet Security scan for the latest viruses or other malicious programs.

Important: Since hundreds of new viruses are discovered every month, we strongly recommend that you regularly update Trend Micro Internet Security.

In addition, as new viruses appear, and existing ones evolve, it becomes necessary to update certain program files and add new functionality to the scan engine. Updating your scan engine ensures Trend Micro Internet Security can act on the new instructions in the virus pattern to detect and remove viruses.

Note: Before you can update Trend Micro Internet Security you must register your software.

To update the virus pattern file and scan engine manually:

1. On the Trend Micro Internet Security Main window, click **Update Now**. The **Manual Update** screen appears. If the Update process doesn't begin, click **Update**. The meter displays the update progress.
2. If you need to halt the update, click **Stop**. To continue updating, click **Update**.

To automatically search for and download the latest pattern, and program files from the Trend Micro ActiveUpdate server, we recommend you schedule the Intelligent Update function. This powerful function keeps Trend Micro Internet Security and all its components updated to offer you maximum protection with minimum user intervention.

To regularly schedule a virus pattern file and scan engine update:

1. On the Trend Micro Internet Security main window, click **Update > Update Setting.**
2. Make sure the **Enable Intelligent Update…** check box is selected, and select how often you want Trend Micro Internet Security to check for updates.
3. Click **Apply**.

Note: To allow Trend Micro Internet Security to automatically perform updates without prompting you first, under **Update Alert**, select the **Automatically update without alerts** check box.

Safer computing practices

Take the following proactive measures to prevent your computer from becoming infected.

☑	**Make sure Real-time Scan is enabled**- Real-time Scan provides constant protection against viruses. With Real-time Scan enabled, you significantly reduce the chance of your computer becoming infected. Because it is so powerful (and because it operates imperceptibly in the background), we recommend that you always keep Real-time Scan enabled.
☑	**Update Trend Micro Internet Security**- Register your software and download the latest versions of the pattern files, scan engine, and program components to ensure Trend Micro Internet Security uses the latest antivirus technology. You should also schedule Trend Micro Internet Security to automatically perform updates using Intelligent Update.

✓	**Beware of suspicious email attachments**- Email is the most common way viruses and malicious code spread. If you receive an email from someone you don't know, you shouldn't save or run any files attached to the email. However, regardless of who sent you the email, be suspicious of email attachments that contain executable files (`.exe`, `.com`).
✓	**Set scheduled scan tasks**- Scan tasks are a quick and easy way to schedule a variety of Manual Scans. Using scan tasks lets you configure the type of files to search and how often to perform the scan. For example, you could set a scan task to scan all types of files on your computer, every Friday night at 10:00 PM.
✓	**Keep informed**- Regularly visit the Trend Micro Web site (`www.trendmicro.com`) for the latest virus information and security alerts. In addition, you can learn more about viruses by accessing the online Trend Micro Virus Encyclopedia.
✓	**Update Microsoft Windows** - Microsoft responds to security issues in their software by releasing patches and other updates on their Web site. Microsoft Windows operating systems provide a Windows update function that allows you to easily download and update these files.

Upgrading your trial version software

Upgrading your 30-day trial version to the full version of the software and registering enables you to use the full functionality of Trend Micro Internet Security.

In addition, after you upgrade your software and register online, you receive the following benefits: the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

If you continue to use the trial version after 30 days all functions are disabled.

If you are using a trial version, on the splash screen, click **Buy Now** and follow the on-screen instructions.

To upgrade your trial version software if you didn't enter a serial number during installation:

1. On the Main window, click **Update > Registration**.
2. Under Step 1 on the Registration screen, type your valid serial number.
3. Click **Upgrade Now**.

You have upgraded your trial version software to the full version. You should now continue and register your software. Refer to *Registering and activating Trend Micro Internet Security* on page 1-8.

Chapter 2

Getting to Know Trend Micro Internet Security

This chapter contains sections that help you become familiar with Trend Micro Internet Security. In addition, it introduces Outbreak Warnings and describes how to access the Trend Micro Internet Security online help.

Included in this chapter are the following sections:

- How Trend Micro Internet Security protects your computer on page 2-2
- Opening the Trend Micro Internet Security main window on page 2-3
- Using the Real-time agent on page 2-6
- Viewing system information on page 2-8
- Introducing Outbreak Warning System on page 2-14
- Accessing online help on page 2-15

How Trend Micro Internet Security protects your computer

Trend Micro Internet Security is designed to protect your computer from both external and internal threats.

Threat	Trend Micro Internet Security Protection
External: viruses and other malicious programs (for example, Trojans, worms), infected email	Real-time Scan is designed to detect and scan any file downloaded, copied or moved to your computer. Mail Scan provides protection from infected incoming and outgoing email messages and attachments, and infected Webmail (Hotmail, AOL Mail, Yahoo! Mail) attachments.
Internal (local machine): viruses and other malicious programs (for example, Trojans, worms)	Manual Scan (on-demand) and Scheduled Scan check your local machine. Trend Micro Internet Security can detect the activity of Trojan horse programs, recover system files that are modified by Trojans, stop their processes, and delete files left behind by Trojans.
Virus Outbreaks	Outbreak Warning System proactively warns you of virus outbreaks or other high-risk situations and advises you to update Trend Micro Internet Security.

Threat	Trend Micro Internet Security Protection
Hackers	The Trend Micro Internet Security firewall provides solid protection from outside intruders, and exception rules for flexibility.
Inappropriate Web sites	URL filter lets you block inappropriate Web sites from loading.
Spam email messages	The Trend Micro Internet Security anti-spam engine identifies spam email messages and tags them so they can be filtered.
Privacy data	Privacy Data Protection allows you to specify personal information (such as your credit card number, or your home address) that Trend Micro Internet Security will block from being transmitted over the Web or in an email message.

Opening the Trend Micro Internet Security main window

The tab interface of Trend Micro Internet Security provides quick access to all areas of your antivirus and Internet security settings.

To view the Trend Micro Internet Security Main window:

- From the Windows taskbar, click **Start** > **Programs** > **Trend Micro Internet Security** > **Trend Micro Internet Security**.

Tip: In the system tray, right-click the Real-time agent and click **Open Main**. (The system tray is next to the clock, on the bottom right hand side of your screen.)

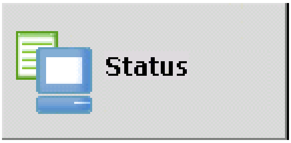
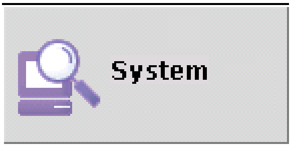
- The Trend Micro Internet Security Main window appears:

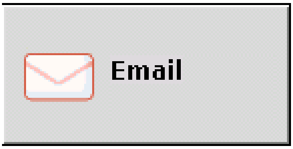
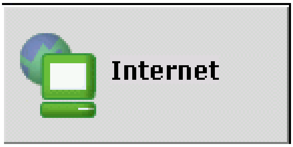
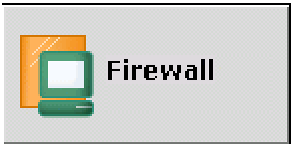
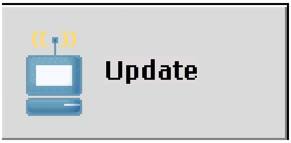
Using Trend Micro Internet Security

The redesigned interface gives you quick access to Trend Micro Internet Security settings and summary information. There are quick links at the top of the Main window for frequently accessed functions:

Quick Link	Description
Update Now	This link immediately checks the Trend Micro ActiveUpdate server for the latest virus pattern file and program updates. The ActiveUpdate server is the Internet server where pattern file and program updates for all Trend Micro products are located. You need to be connected to the Internet for update functionality.
Scan Now	Scans your system, according to your specified Manual Scan settings.
Help	Allows you to view the Online Help, Virus Encyclopedia and Virus Information Center, and the Trend Micro Home Page.

Each of the buttons on the right hand side of the interface lets you view or manage the settings for a particular security or antivirus area.

To perform the following action:	Click:
View the system status and event logs.	
View your antivirus settings and quarantine files, or perform a scan task.	

To perform the following action:	Click:
View your Mail Scan, Web Scan, and Anti-spam settings.	
View your URL filter and Privacy Data Protection settings.	
View your Personal Firewall profile settings.	
View your update settings, or perform a manual update. Register your software.	

Using the Real-time agent

The Real-time agent is the program that provides real-time protection of your computer. The Real-time agent is the quickest way to access certain functions, for example to display the Main window.

Starting the Real-time agent

The Real-time agent is configured to automatically launch and appear in your system tray each time your computer starts up. However, if you do not see the Real-time agent in your system tray, we recommend you launch it.

To start the Real-time agent:

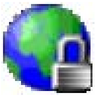
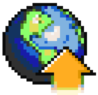
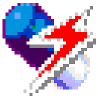
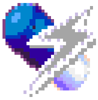
- From the Windows taskbar, click **Start** > **Programs** > **Trend Micro Internet Security** > **Real-time Agent**.

With the Real-time agent, you know at a glance if Real-time Scan is enabled or disabled.

To:	Do the following:
Open the Main window	Double-click the Real-time agent.
Turn off the Real-time agent	Right-click the Real-time agent and click **Exit**. **Important:** If you turn off the Real-time agent, Real-time Scan will also be disabled.
Halt all Internet Traffic	Right-click the Real-time agent and click **Emergency Lock**.
Perform an update	Right-click the Real-time agent and click **Update Now**.

Identifying Real-time agent icons

Use the table below to learn the meanings of Real-time agent icons.

Icon	Description
	All incoming and outgoing Internet traffic has been stopped (to allow Internet traffic, refer to *Using the Emergency Lock* on page 5-3).
	Connecting to the Trend Micro server to download the latest updates.
	Real-time Scan is enabled (red lightning bolt).
	Real-time Scan is disabled (grey lightning bolt). To enable Real-time Scan, refer to *Confirming Real-time Scan is enabled* on page 3-1.

Viewing system information

Both summary and detailed information about your antivirus and Internet security is available through Trend Micro Internet Security. You can view summary information to quickly check which settings are enabled, or you can view the logs for details of security, antivirus, and program events.

Viewing product information

It is important to make sure your pattern files and scan engine are kept up to date. Using the latest version of these components ensures you have the most updated virus protection Trend Micro can offer. To confirm you have the latest updates, you can view your current pattern file and scan engine version.

To view important product information:

- Click **Help** > **About Product** > **Version Information**.

Your serial number is also displayed. If you contact technical support or an authorized reseller for help with an issue or to re-install Trend Micro Internet Security, you need your serial number.

You can check the latest available pattern file and scan engine versions by visiting the Trend Micro Virus Information Center.

To visit the Trend Micro Virus Information Center:

- Click **Help** > **Virus Information Center.**

Viewing Internet Security status

The Internet Security status window provides a quick overview of the status of your Internet security. It allows you to quickly assess whether your system is secured in the following areas: Personal firewall, URL filter, Privacy Data Protection, and Anti-spam.

To view Internet Security status:

- Click **Status > Internet Security Status**.

Current Status provides an overview of the health of your Internet security:

Current Status	Meaning
Normal	Personal Firewall, Privacy Data Protection, and Anti-spam are enabled.
Caution	Some of the Trend Micro Internet Security settings are disabled. Check the Setting status box for more information.
Unsafe	Some of the Trend Micro Internet Security settings are disabled. Your system may be unsafe. Check the **Setting status** box to view and re-enable the disabled settings.

The **Last attack information** box shows the most recent attempt to attack or scan your computer. This information is only applicable if your Personal Firewall is enabled.

The **Setting status** box shows the current enabled/disabled status of the Internet security settings. Click the link to display the configuration window for each setting.

The **Internet traffic monitor** box displays the total amount of traffic received and sent. An increase in sent or received traffic when you are not using any Internet services may indicate Trojan or virus activity.

Viewing Antivirus status

The Antivirus status window provides a summary of your antivirus scanning and update settings. Use this page to check the overall status of your antivirus settings, and to view antivirus statistics.

To view the Antivirus status:

- Click **Status** > **Antivirus Status**.

Current Status provides an overview of the health of your antivirus settings:

Current Status	Icon Meaning
Normal	Real-time Scan, Incoming Mail Scan, Outgoing Mail Scan, Webmail Scan, and Intelligent Update are enabled
Caution	One or more of the antivirus settings are disabled. Check the **Update and scan settings** box for more information.
Unsafe	All your antivirus settings are disabled. Your system may be unsafe. Check the **Update and scan settings** box to view and re-enable the disabled settings.

The **Scan and virus status** box shows information about the last virus and infected file found, the last file scanned, and the times of your last manual and scheduled scans.

The **Update and scan settings** box shows the current enabled/disabled status of the antivirus security settings. Click the link to display the configuration window for each setting.

Viewing Event logs

Trend Micro Internet Security keeps logs for all update, virus, URL filter, Damage Cleanup Service, Privacy Data Filter, Anti-spam, and Personal Firewall events. These logs can be viewed from the Event logs screen and provide a valuable source of information. For example, you can view the virus type to learn if it is a Trojan or a worm and should be deleted rather than quarantined.

In addition to displaying the date and the time of each recorded log, the various log types provide log-specific information.

Log	Entries are created when:
Update	You try to download the latest components. Update log entries also contain what file(s) were downloaded and installed from Trend Micro and the status—Successful or Unsuccessful--of the download.
Virus	A virus or other malicious program is detected. Virus log entries also contain the time the virus was detected; the type of scan--Real-time or Manual--that detected the virus, the source type of the virus, the name of the virus, the name of the file that contains the virus, the status of the first action, and if applicable the status of the second action.
Damage Cleanup Service	A Trojan is detected by the Trend Micro Damage Cleanup Service (DCS). DCS detects and cleans Trojan horse viruses. DCS log entries contain the time the Trojan was detected, the name of the Trojan, and the result of the cleaning action.

Log	Entries are created when:
URL filter	A Web site is blocked or harmful Web content is encountered. URL filter log entries also contain the time at which access to a restricted site was attempted, the URL, or Web address that was blocked, and the action URL filter performed.
Personal Firewall	Your computer experiences an attack from the Internet. Personal Firewall log entries also contain the type of firewall defense, time of the attack, direction of network traffic, type of protocol used, source IP address, source port number, destination IP address, destination port number, and the reason traffic was blocked.
Privacy Data Protection	Your computer attempts to send your private data over the Internet. Privacy Data Protection log entries contain the time of the attempt to send privacy data, the type of data, and the web site or the email address of where the data was being sent.
Anti-spam	When spam is identified and tagged. Anti-spam logs contain the time of the detection, the subject of the email, and the sender of the email.

To check your logs:

1. On the Main window, click **Status > Event Logs.**
2. Click the type of log you want to view.
3. Click **View Logs**.
4. Select the date of the log you want to view.

Note: To sort the logs (ascending or descending) by column header (for example: Time), click the column title.

Introducing Outbreak Warning System

Trend Micro Internet Security includes an innovative service to prevent the latest virus outbreaks or other malicious threats. Leveraging the research and knowledge of Trend Micro TrendLabs, Trend Micro Internet Security can proactively warn you in advance of threats so you have time to update your software to prevent infection. (TrendLabs is the Trend Micro global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.)

The Outbreak Warning system must be enabled before you will receive Outbreak Warnings.

To enable Outbreak Warning System:

1. From the Windows taskbar, click **Start** > **Programs** > **Trend Micro Internet Security** > **Outbreak Warning Settings**.
2. Select the **Enable Outbreak Agent to provide proactive recommendations** check box.
3. To view the most recent Outbreak Warning, click **View Alert**.
4. Click **OK**.

Outbreak Warnings are classified as Red and Yellow Alerts. Red Alerts correspond to the TrendLabs High-Risk ranking and Yellow Alerts to the Medium-Risk ranking.

Important: If you receive an Outbreak Warning, the first thing you should do is update your virus pattern file and scan engine, and then run a scan on your entire computer.

High-Risk Criteria (Red Alert)	**Medium-Risk Criteria (Yellow Alert)**
Several infection reports reporting rapidly spreading malware. The industry's first 45-minute Red Alert solution process is started: An official pattern release (OPR) is deployed with notification of its availability and any other relevant notifications are sent out.	Infection reports are received from several business units (BUs) as well as support calls confirming scattered instances, and an OPR is made available for download.

Accessing online help

The Trend Micro Internet Security online help provides comprehensive coverage of all the functions and features of Trend Micro Internet Security. Use the online help to find the answers for your Trend Micro Internet Security questions.

To access online help:

- On the Trend Micro Internet Security Main window, click **Help** > **Contents and Index**. The online help appears.

In addition, when you are using the program you may also see Help buttons. Click these buttons to view context-sensitive help (relevant help information based on what you are currently viewing).

Chapter 3

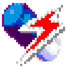
Protecting Your Files and Data

This chapter contains information about basic tasks you should perform to protect your computer. It includes the following sections:

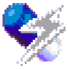
Confirming Real-time Scan is enabled

Real-time Scan provides constant protection against viruses by scanning files that are copied, downloaded, or moved to your computer. Real-time scanning takes place in the background and requires no user intervention, so you don't really have to do anything to "use" Real-time Scan--just be sure it is enabled.

You can check if Real-time Scan is enabled (which it is by default) by looking at the Real-time agent in the Windows system tray.



Enabled (default) red lightning bolt



Disabled grey lightning bolt

Important: If you turn off the Real-time agent, Real-time Scan will also be disabled.

To enable Real-time Scan:

- In the system tray, right-click the Real-time agent, and then click **Real-time Scan**.

Confirming Mail Scan is enabled

Email is the most common way for viruses and other malicious programs to spread and opening an infected email or attachments is the primary means of virus infection. Due to the popularity of email communication, virus writers create viruses that exploit the vulnerabilities of email client software.

Mail Scan is designed to check email messages and attachments as they are downloaded and sent from an Internet (POP3/SMTP) mail server. Supported email clients are:

- Microsoft Outlook 2000 and above
- Outlook Express 5.5 and above
- Eudora Pro 5.0 and above
- Netscape Messenger 7.0 and above

Mail Scan can also scan mail attachments downloaded from a Webmail account (email stored on a server and accessed by a Web browser). Supported Web mail accounts are:

- Microsoft Hotmail

- Yahoo! Mail
- AOL Mail

Trend Micro Internet Security Mail Scan must be enabled before your email messages will be scanned.

To confirm Mail Scan is enabled:

1. On the Main window, click **Email > Mail Scan**.
2. Click **Incoming Mail**. Ensure the **Enable incoming mail scanning** check box is selected.
3. Click **Outgoing Mail**. Ensure the **Enable outgoing mail scanning** check box is selected.
4. Click **Apply**.

Scanning your entire computer

Scan all drives to check if your computer is infected. With one click, Trend Micro Internet Security provides a fast and easy way to scan all drives connected to your computer for infected files.

To scan your entire computer:

- On the Main window, click **Scan Now**. The Scan Files dialog box appears and Trend Micro Internet Security begins scanning. To stop scanning, click **Stop**. A confirmation message box appears. Click **Yes** to confirm and then click **OK**.

Note: Trend Micro Internet Security scans the file types and executes the necessary scan actions according to the Manual Scan settings. To change these settings, refer to the online help under the book "Configuring Virus Scan settings".

Scanning a folder or file

With Trend Micro Internet Security, you can scan the entire contents of a folder, including subfolders, or you can scan a single file. Trend Micro

Internet Security scans the file types and executes the necessary virus actions according to the Manual Scan settings.

To scan a folder:

- Right-click the folder, and then click **Scan Virus**.

Tip: You can also "drag" the folder onto the Trend Micro Internet Security Main window.

To scan a single file:

- Right-click the file, and then click **Scan Virus**.

Tip: You can also right-click the file, select **Properties**, then click the **Virus Property** tab; or you can "drag" the file onto the Trend Micro Internet Security Main window.

Running scan tasks

Scan tasks let you schedule a variety of scans to automatically run at the specified time. For example, you could create a scan task that checked all file types on all your drives, every Friday at 10:00 PM. However, at any time you can manually execute previously defined scan tasks.

Trend Micro Internet Security provides a number of pre-defined scan tasks. In addition to running these scan tasks, you can also view them to give you hints about how to create your own effective scan tasks.

To run a scan task:

1. On the Main window, click **System > Scan Files**.
2. Select the task you want to execute.
3. Click **Scan**. To stop scanning, click **Stop**. A confirmation dialog box appears Click **Yes** to confirm and then click **OK**.

Note: To learn more about scan tasks, refer to the online help under the book "Managing Scan Tasks".

Blocking spyware

Trend Micro Internet Security blocks spyware from being installed on your computer, by including spyware in Real-time Scan. Spyware is software that is installed with legitimate programs or utilities, or may be installed after visiting a Web site. Companies bundle spyware with programs mostly to collect personal information, including the Web sites you visit, how long you spend at a certain Web site, or information about your local machine. While most of the shareware or freeware software downloaded from the Internet does not contain spyware, there is still a significant number of companies that do bundle spyware with their programs.

To enable spyware blocking:

1. On the Trend Micro Internet Security main window, click **System > Scan Settings.**
2. Click **Real-time Scan**.
3. Select the **Scan for spyware** check box.
4. Click **Apply**.

Searching for and cleaning Trojans

Trend Micro Internet Security detects Trojan activity, recovers files modified by the Trojan, stops Trojan processes, and deletes files left behind.

Trojans, or Trojan horses, are small, seemingly harmless programs. To cause any damage, these programs must be installed onto your system. Once a Trojan is installed, it has all the same privileges as the user of the computer and can exploit the system to do something the user did not intend. The main difference between Trojans and viruses is that Trojans cannot replicate or spread on their own.

Trend Micro Internet Security searches for Trojans during initial installation, and you can configure Trend Micro Internet Security to automatically search for Trojans during manual scans and every time Real-time Scan starts.

To automatically search for and delete Trojans during scans:

1. On the Trend Micro Internet Security main window, click **System > Scan Settings**.

2. Click **Manual Scan** or **Real-time Scan**, depending on which scan you also want to include searches for Trojans. Trend Micro recommends including searches for Trojans for both Manual and Real-time Scan.
3. Select the **Search for and clean Trojans** check box.
4. Click **Apply**.

However, you can also manually search for Trojans.

To manually search for and delete Trojans:

1. Locate the folder where you installed Trend Micro Internet Security (for example, the default location is C:\Program Files\Trend Micro\Internet Security).
2. Double-click the **Tsc.exe** file.

Protecting your private data

Privacy Data Protection allows you to define certain types of information (for example, your name, address, or credit card number) which will then be blocked from being sent over the Web or in email messages.

Note: You must define your private data before the Privacy Data Protection feature will function. See the online help under the book "Protecting Private Data" for more information.

To confirm Privacy Data Protection is enabled:

1. On the Main window, click **Internet** > **Privacy Data Protection**.
2. Ensure the **Enable Privacy Data Protection** check box is selected.
3. Click **Apply**.

To add or edit a Privacy Data Protection item:

1. On the Main window, click **Internet** > **Privacy Data Protection**.
2. Choose one of the following:
   - To add a new item, click **Add**.
   - To edit an existing item, select the existing item, and then click **Edit**.
3. Type a name and description for the item in the **Item name** and **Description** boxes.

4. Type your privacy data in the **Privacy data** box. Trend Micro Internet Security will match the data exactly as you type it. Note that the information you type is case-sensitive, so *trend*, *TREND*, and *tReNd* are all considered different.
5. Choose one or both of the following:
   - To protect this item from being sent over the Web, select the **Check Web protocol** check box.
   - To protect this item from being sent via email, select the **Check mail protocol** check box.
6. Click **OK**. The item is saved.

Reducing spam

Spam email messages (also known as junk email) are an expensive and annoying problem on the Internet. The Trend Micro Internet Security anti-spam engine identifies spam email messages and adds an identifier tag so they can be easily identified or filtered.

The anti-spam feature must be enabled on the computer before spam is tagged.

To confirm anti-spam is enabled:

1. On the Trend Micro Internet Security main window, click **Email > Anti-spam**.
2. Ensure the **Enable Anti-spam** check box is selected.

You can configure Trend Micro Internet Security Anti-spam to operate on three different levels. On the highest level, the anti-spam rules are very strict. This leads to more spam being correctly identified, however legitimate email messages are more likely to be incorrectly tagged. The lowest level has much looser anti-spam rules. This leads to more spam getting through, but less chance of legitimate email messages being falsely tagged.

When an email message is identified as spam, the Subject line will be modified with "SPAM: " at the front. Set up a rule in your email client to filter these messages to a special "spam" folder, where you can periodically check for any legitimate email that was incorrectly tagged. (See your email client documentation for information on setting up rules.)

Anti-spam also has an approved senders list, which enables you to specify known email addresses. Any email messages originating from an email address on the approved senders list will not be tagged as spam.

To configure anti-spam settings:

1. On the Main window, click **Email > Anti-spam**.
2. Choose a setting from the **Anti-spam level** slider.
3. To add email addresses to your approved senders list, click **Edit White List...**
   - To add a new email address to the approved senders list, click **Add**. Type the email address, and then click **OK**.
   - To delete an email address from the approved senders list, highlight the address in the list and click **Delete**.
4. Click **OK**.

Note: Email messages larger than the limit specified for the incoming (POP3) mail scan will not be filtered for spam.

Chapter 4

Dealing with Viruses

With the number of viruses already “in-the-wild” and the number of viruses created and released, it is likely you will encounter a virus at some point. This chapter contains the following sections:

- Understanding Trojans on page 4-1
- Understanding viruses on page 4-1
- What to do when a virus is detected on page 4-2
- Actions on uncleanable files on page 4-2
- Cleaning boot viruses on page 4-3

Understanding Trojans

Trojans, or Trojan horses, are small, seemingly harmless programs. To cause damage, these programs must be installed onto your system. Once installed, a Trojan has complete access to your data files, and can take complete control of the system. The main difference between a Trojan and a virus is that Trojans cannot replicate or spread on their own.

Understanding viruses

Simply put, a computer virus is a program that replicates. To do so, it will need to attach itself to other program files (for example, `.exe`, `.com`, `.dll`) and execute whenever the host program executes. Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage.

Called the damage routine, or payload, the destructive portion of a virus can range from overwriting critical information stored on your hard disk's partition table to scrambling the numbers in your spreadsheets to just taunting you with sounds, pictures, or obnoxious effects.

To learn more about any particular virus, or about viruses in general, you can access the Trend Micro online Virus Encyclopedia or visit our Web site at:

`www.trendmicro.com.`

What to do when a virus is detected

First, do not panic. When Trend Micro Internet Security detects a virus either by Real-time, Manual, or Mail Scan, Trend Micro Internet Security notifies you of the virus and the scan action performed.

For Real-time and Mail Scan a message box is displayed describing the infected file and the scan action performed.

The scan actions for Real-time, Manual, or Mail Scan depend on the settings you have configured for each scan. However, the default action for all scans is Clean.

This simply means if a file becomes infected, Trend Micro Internet Security first attempts to clean the file. The default secondary action for Real-time and Manual Scan is Quarantine.

Trend Micro Internet Security may detect a malicious program which cannot be cleaned. Some malicious programs (such as Trojans and worms) do not infect files, so therefore cannot be cleaned. Also, certain types of viruses overwrite existing data, making cleaning impossible. By default, Trend Micro Internet Security moves these "uncleanable" files to the Quarantine folder. (The default secondary action for Mail Scan is Delete.)

Actions on uncleanable files

Quarantined malicious programs cannot be cleaned, as they are programs. No virus is infecting a file, rather the entire program itself needs to be "cleaned". Any malicious programs that are quarantined should be deleted.

For more information about how to handle files in the Quarantine Folder, view the interactive Quarantine Guide.

To view the Quarantine Guide:

1. On the Main window, click **System > Quarantine**.
2. Click **Quarantine Guide** and follow the instructions.

You can learn the virus type by viewing the Virus logs. The following provides further information about how to identify different types of viruses based on their name.

Type of malicious program	Name prefix	Example
Trojan horses	TROJ_<name>	TROJ_QAZ.A
Worms	WORM_<name>	WORM_KLEZ
Script Viruses	VBS_<name> JS_<name>	VBS_BRITNEYPIC.A
File infecting viruses	PE_<name>	PE_VETTIKINS.A
Spyware	SPYW_<name>	SPYW_NARGON.A

Cleaning boot viruses

Boot sector viruses are especially troublesome (and dangerous) because they occupy a sensitive part of the hard drive, the boot sector, and load into memory whenever the system is started. From memory, they spread easily to any files that are subsequently opened and to floppy disks that are used.

Trend Micro Internet Security automatically scans for boot sector viruses during a manual or scheduled scan. If a boot sector virus is found, Trend Micro Internet Security performs the action specified for the current scan.

Note: Boot viruses spread easily. If Trend Micro Internet Security detects a boot virus, it is very likely that one or more of your floppy disks are also infected. Be sure to run the Floppy Scan task and check all your floppies for viruses.

Chapter 5

Guarding Your Internet Connection

This chapter includes instructions on how to secure your Internet connection from malicious hackers. It also describes how you can prevent Web sites from being viewed using the URL filter.

This chapter contains the following sections:

- Introducing the Personal Firewall on page 5-1
- Using the Emergency Lock on page 5-3
- Blocking network viruses on page 5-4
- Filtering unwanted Web content on page 5-4

Introducing the Personal Firewall

The Trend Micro Internet Security Personal Firewall protects your computer against attacks from the Internet. A firewall creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters the incoming and outgoing Internet traffic. By filtering Internet traffic, the firewall helps prevent malicious hackers from invading your computer and causing mischief.

The Trend Micro Internet Security firewall is a "stateful inspection" firewall which means it tracks and monitors the state of each connection to make sure nothing strange is going on. For example, stateful inspection would know if something other than HTTP was running over port 80. A stateful inspection firewall keeps track of each "session" and knows if the session is already active. The firewall uses this information plus a list of rules to determine if a packet (which is the basic unit of data transferred across a network) is blocked or forwarded.

Filtering decisions are based not only on defined rules, but also on context that has been established by prior packets that have already passed through the firewall.

The Personal Firewall includes the following features:

- Ability to allow or deny traffic based on a specified port or protocol
- Displays a dynamic outgoing access warning when a program that is not included in the exception list tries to connect to the Internet (High security level only)—this warning helps prevent unauthorized programs such as a Trojans from stealing data or someone from remotely controlling your computer
- Uses an IDS (Intrusion Detection System) to prevents known firewall attacks
- Provides updateable firewall and IDS rules
- Ability to filter HTTP strings from server-to-server to prevent hybrid attacks like Nimda and Code Red

Enabling the Personal Firewall

Enable your Personal Firewall so you can connect to the Internet without worrying about someone invading your computer. The Personal Firewall protects you against hackers trying to damage files, steal personal information, or create mischief.

To confirm the Personal Firewall is enabled:

1. On the Trend Micro Internet Security Main window, click **Firewall > Firewall Profiles.**
2. Ensure that the **Enable Personal Firewall** check box is enabled.
3. Click **Apply**.

Understanding Personal Firewall profiles

Trend Micro Internet Security allows you to configure different Personal Firewall profiles for different situations. Depending on your computer and network settings, you may require certain ports or services enabled in some situations. By using Personal Firewall profiles, you can easily switch profiles between, for example, a home network and a wireless LAN, thereby keeping your security as tight as possible. The Personal Firewall comes configured with a variety of common network configurations. You can use one of these configurations without modification, or you can create and customize your own profile.

Note: See the online help under "Managing Personal Firewall Profiles" for more information.

Using the Emergency Lock

Complete control over your Internet traffic is vital for virus outbreaks or other intrusion attacks. The Emergency Lock immediately stops all incoming and outgoing Internet traffic and is particularly useful during times when someone is trying to remotely break into your computer or there is a virus outbreak.

To activate the Emergency Lock:

- On the Main window, click **Status > Internet Security Status**, and then click **Emergency Lock**. All Internet traffic is now halted, so you will not be able to browse the Web or check your email messages until the Emergency Lock is deactivated.

To deactivate the Emergency Lock:

- Click **Emergency Lock** again.

Tip: In the system tray, right-click the Real-time agent icon and click **Emergency Lock** or when Real-time Scan detects a virus click **Emergency Lock** on the message box that appears.

Blocking network viruses

Network viruses such as NIMDA spread rapidly through the Internet and local networks. Trend Micro Internet Security helps prevent your computer from being infected by network viruses, and prevents your computer from infecting other computers. Trend Micro Internet Security can do the following upon detection of a network virus:

- Halt all Internet traffic immediately
- Pop-up a Red Alert message

To view information about network viruses:

1. On the Trend Micro Internet Security Main window, click **Firewall > Network Virus Emergency Center**.
2. Click the link for more information about a particular network virus.

To change network virus settings:

1. On the Trend Micro Internet Security Main window, click **Firewall > Network Virus Emergency Center**.
2. Do one of the following:
   - To immediately halt Internet traffic when a network virus is detected, click **Halt all Internet traffic when network virus detected** check box.
   - To display an alert when a network virus is detected, select the **Display Red Alert pop-up** check box.
3. Click **Apply**.

Filtering unwanted Web content

For protection against offensive Web content, Trend Micro Internet Security offers the URL filter. This feature lets you set whatever Web sites you want "off-limits" to other users of the computer.

The URL filter can work in two different modes:

- Enable access to all Web sites by default. You then specify a list of sites you do NOT want access to. This list of URLs is known as the restricted list.

- Disable access to all Web sites by default. You then specify a list of sites you DO want access to. This list of URLs is known as the permitted list.

To filter unwanted Web content:

1. On the Trend Micro Internet Security Main window, click **Internet > URL Filter**
2. Select the **Enable URL filtering** check box.
3. Click **Apply**.

A Trend Micro Internet Security "Blocked URL" message will be displayed when someone attempts to access a blocked Web site.

To add or edit a Restricted or Permitted List URL:

1. On the Trend Micro Internet Security main window, click **Internet > URL Filter.**
2. Choose one of the following:
   - To allow access, click **Allow access...**. Your Restricted List is now operational.
   - To block access, click **Block access...**. Your Permitted List is now operational.
3. Do one of the following:
   - To add a new URL: click **Add**.
   - To edit a URL: select the URL, and then click **Edit**.
4. You can either add a URL manually, or retrieve URLs from your browser favorites or cache. Importing URLs from your browser cache is a quick way to add all your recently accessed Web sites to the Permitted List. To add a URL manually:
   - In **Add the URL**, type the URL of the blocked (Restricted List) or allowed (Permitted List) Web site. For example, www.somewebpage.com.
5. To add all the URLs from your browser cache:
   - Click **Import URLs from Web browser cache**. If you would prefer to import your URLs from your browsers favorites, click **Import My Favorites**.
6. To block the entire Web site including all sub-pages, select the **Include all sub-pages...** check box.

7. Click **OK**. If you selected the **Include all sub-pages...** check box, a small cross appears on the URL icon.
8. Click **Apply**.

Chapter 6

Getting Support

Trend Micro is committed to providing service and support that exceeds our user's expectations regardless of their location. This chapter contains information on how to get technical support. You must register your product to be eligible for support.

The following topics are discussed in this section:

- Before contacting Technical Support on page 6-1
- Visiting the Customer Care Center on page 6-2
- Visiting the Technical Support Web site on page 6-2
- Contacting Technical Support on page 6-2
- TrendLabs™ on page 6-3
- Sending your infected files to Trend Micro on page 6-3

Before contacting Technical Support

Check your documentation: the manual and online help provide comprehensive information about Trend Micro Internet Security. Search both documents to see if they contain the solution to your problem.

Visit our Technical Support Web site: our Technical Support Web site contains the latest information about all Trend Micro products. Previous user inquiries that have been answered are posted on the support Web site.

Visiting the Customer Care Center

The Customer Care Center contains the latest news about Trend Micro Internet Security. As a registered user, you can access information that is not available outside this Web site.

To visit the Trend Micro Customer Care Center:

- On the Main window, click **Help** > **Customer Care Center**.

Visiting the Technical Support Web site

Visit the Trend Micro Technical Support Web site to find answers to your inquiries. The Trend Micro Technical Support Web site contains the latest updated information about our products. New solutions are added daily. However, if you don't find the answer you seek, you can submit your question on-line, where the experts at TrendLabs will provide you with an answer or contact you for more information.

To visit the Technical Support Web site:

- On the Main window, click **Help** > **Technical Support Home Page**.

Contacting Technical Support

A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product serial number
- Trend Micro Internet Security program, scan engine, pattern file, version number
- Operating System name and version and Internet connection type
- Exact text of any error message given
- Steps to reproduce the problem

The best way to receive support is to send an email to our highly trained Technical Support staff or visit our Web site.
`Email: support@trendmicro.com`

For other ways to contact Technical Support, check the "Support" section of our Web site at:
`URL: www.trendmicro.com`

TrendLabs™

Trend Micro TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:
`www.trendmicro.com/en/security/trendlabs/overview.htm`

Sending your infected files to Trend Micro

You can send your viruses to Trend Micro via the Web. More specifically, if you have a file that you think is infected with a virus but our scan engine does not detect it or cannot clean it, we encourage you to submit the suspicious file to us at the following Web address:
`http://subwiz.trendmicro.com`

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any virus(es) it may contain and return the cleaned file to you usually within 48 hours.

Appendix

This appendix contains information that may not be applicable for all users. It includes the following sections:

- Working with rescue disks on page A-1
- Enabling and configuring proxy settings on page A-3

Working with rescue disks

Certain types of boot viruses can prevent your computer from booting normally. To clean these viruses, you need to start your computer from a clean disk and not the infected hard drive. A "rescue disk" is a bootable floppy disk that Trend Micro Internet Security can create if you are running Microsoft Windows 98 or Windows Me.

The Trend Micro Internet Security rescue disks require a "pure DOS" environment to operate correctly, however Windows 2000 and XP no longer support a pure DOS environment.

For Windows 2000 and XP we recommend you create an Emergency Repair Disk. Refer to the Microsoft Windows documentation for instructions.

You need multiple disks to create the complete set of rescue disks.

Note: Rescue disks should be write protected after they are created. A disk is write protected when you can see through both squares in the upper corners.

- Emergency Boot Disk (Disk 1): Contains files necessary to start your computer. Use to start your computer if a boot virus has infected your computer and you cannot start your computer normally.
- PCSCAN Files Disk (Disk 2): Contains the scan engine. Use with the Pattern File disks to detect and clean viruses located in the boot sector of your computer.
- Pattern File Disks (Disks 3 and others): Contains pattern files to detect the latest viruses. Use with the PCSCAN Files disk to detect and clean viruses located in the boot sector of your computer.

Note: Do not restart your computer using rescue disks that were created for an earlier version of Trend Micro PC-cillin-- this can result in data loss.

Before creating your rescue disks make sure you have a writing utensil to label the disks. You need at least seven disks to create a complete set of rescue disks.

If you've already got a set of rescue disks from a previous version of Trend Micro software, you should create a new set after installing Trend Micro Internet Security. Likewise, if you created your rescue disks under Windows 98 and have upgraded to Windows Me, you need to create a new set of rescue disks. Of course, you can re-use your old floppies for the new disks. All data on the old disks will be lost in the creation of the new disks.

To create rescue disks:

1. Obtain some disks and insert one into the floppy drive of your computer.
2. From the Windows taskbar, click **Start** > **Programs** > **Trend Micro Internet Security** > **Create the Rescue Disks**. The Create Emergency Rescue Disks window appears.
3. Click **Complete Rescue Disk set**, and then **Click Next**.
4. Make sure the Target drive is correct and click **Next**. The Format dialog box appears.
5. Choose your format type (we recommend Full) and click **Start**. The disk starts formatting.
6. When the formatting is finished, click **Close**. The Format dialog box closes and Trend Micro Internet Security starts copying the files to the disk.

7. As each floppy is finished, remove it and immediately label it. Slide up the plastic button in the upper left hand corner of the back of the disk to write protect it. The disk is write-protected when you can see through both squares in the upper corners. Creating the rescue disks takes about 10 minutes.
8. Repeat the procedure for each disk, starting from the formatting step.
9. Click **Finish**.

Note: You cannot make rescue disks on a machine infected with a boot virus. Be sure to clean (or delete) any viruses that have been detected.

Enabling and configuring proxy settings

A proxy server is used to provide security and increase efficient use of network bandwidth. Most home users do not use a proxy server, but many offices and schools do. If you are having trouble connecting to the Internet to register, or download program updates, it may be because you use a proxy server but it has not been identified or there is an error in the address/credentials.

If you use a proxy server on your network you need to enter the IP address (number) and port of this proxy server.

In addition, if you use a proxy server and users are required to log on, you need to supply the appropriate logon credentials.

To enable and configure proxy settings:

1. On the Main window, click **Update > Update Setting**.
2. Under **Proxy information**, select the **Use a proxy server...** check box.
3. Click **Proxy Settings**, and then do the following:
    - Type the IP address of the proxy server or domain name (for example, `proxy.yourcompany.com`).
    - Type the port number of the proxy server (for example, 80).
    - If necessary, type your proxy server logon credentials.
4. Click **OK**.
5. Click **Apply.**

Index